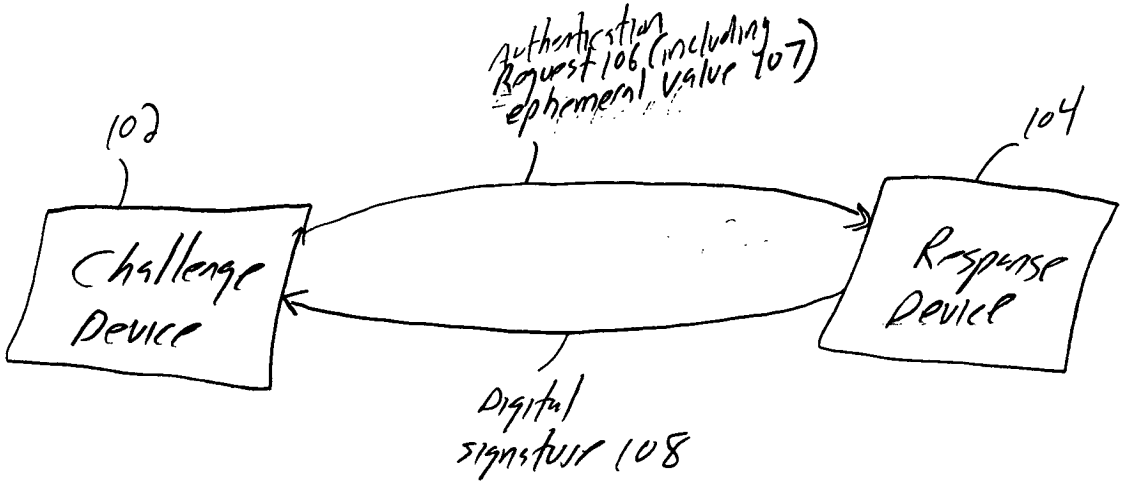
Authentication Request 106 (including ephemeral value 107)
102
104
Challenge Device
Response Device
Digital signature 108

FIG. 1

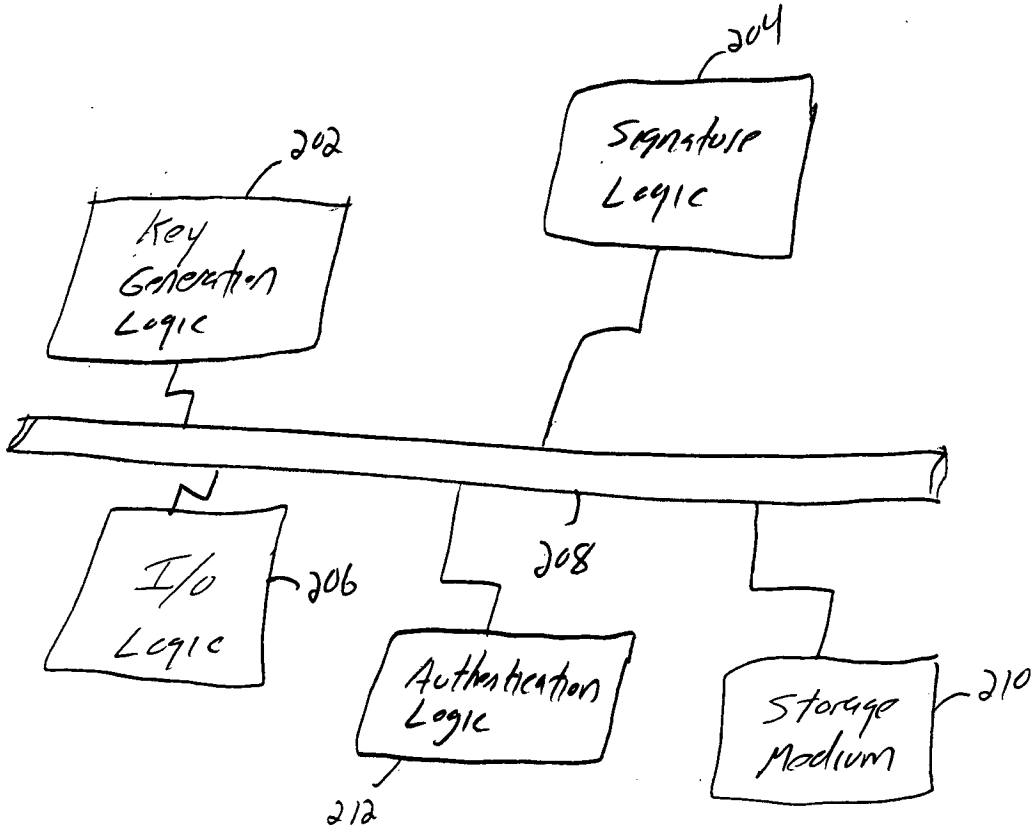
Challenger Device
102
204
Signature Logic
202
Key Generation Logic
I/O Logic
206
208
Authentication Logic
212
Storage Medium
210

FIG. 2

Response Device 104

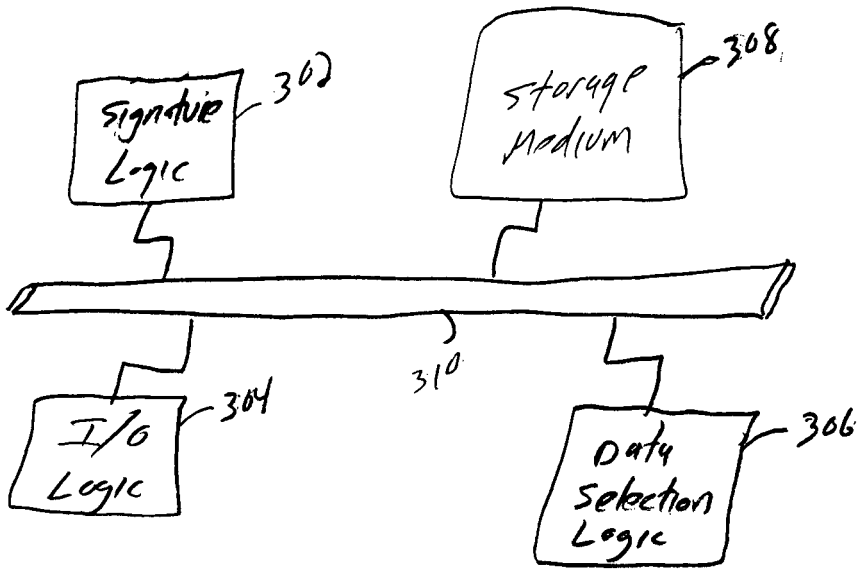

FIG. 3

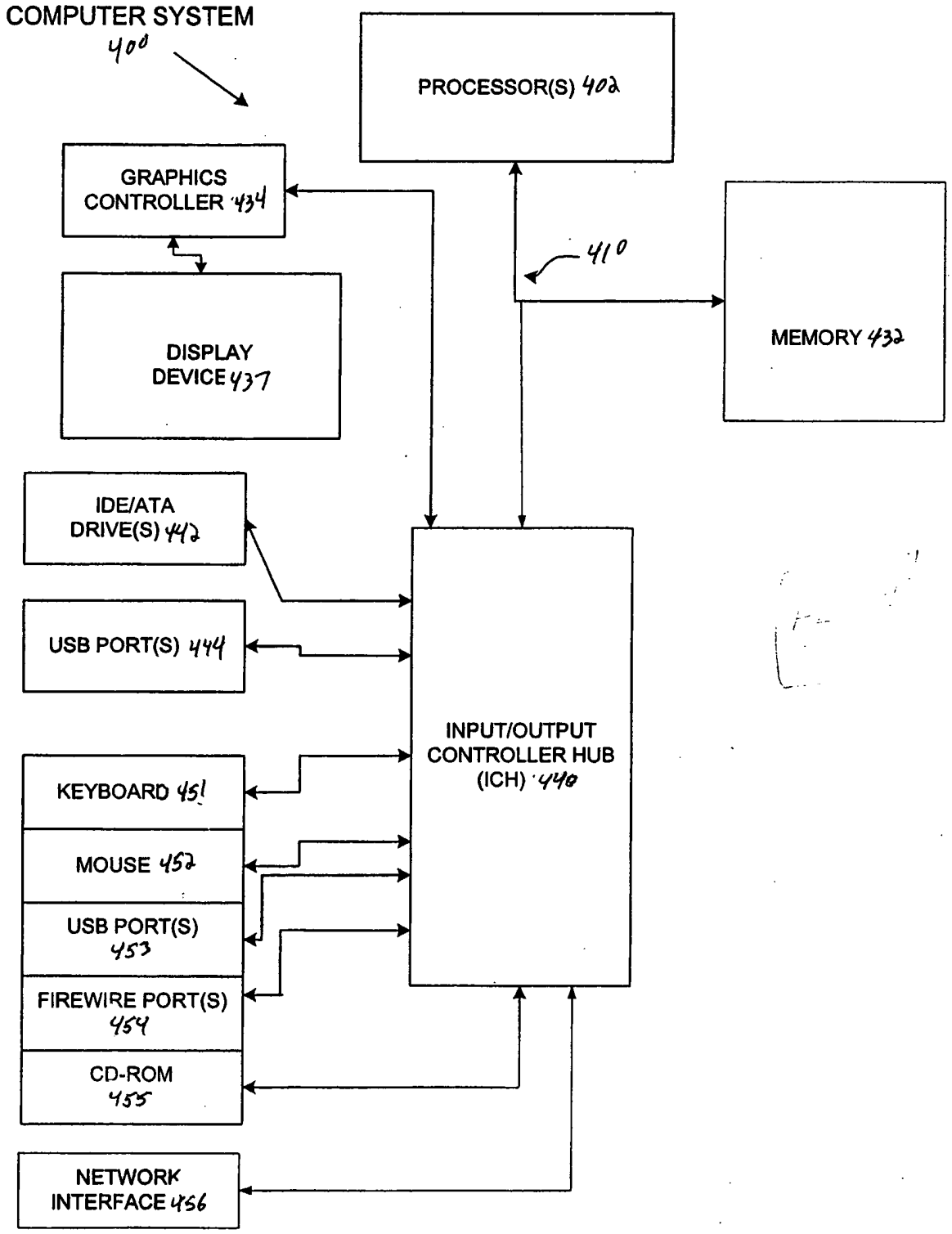
COMPUTER SYSTEM
400
PROCESSOR(S) 402
GRAPHICS CONTROLLER 434
410
MEMORY 432
DISPLAY DEVICE 437
IDE/ATA DRIVE(S) 442
USB PORT(S) 444
INPUT/OUTPUT CONTROLLER HUB (ICH) 440
KEYBOARD 451
MOUSE 452
USB PORT(S) 453
FIREWIRE PORT(S) 454
CD-ROM 455
NETWORK INTERFACE 456

FIG. 4

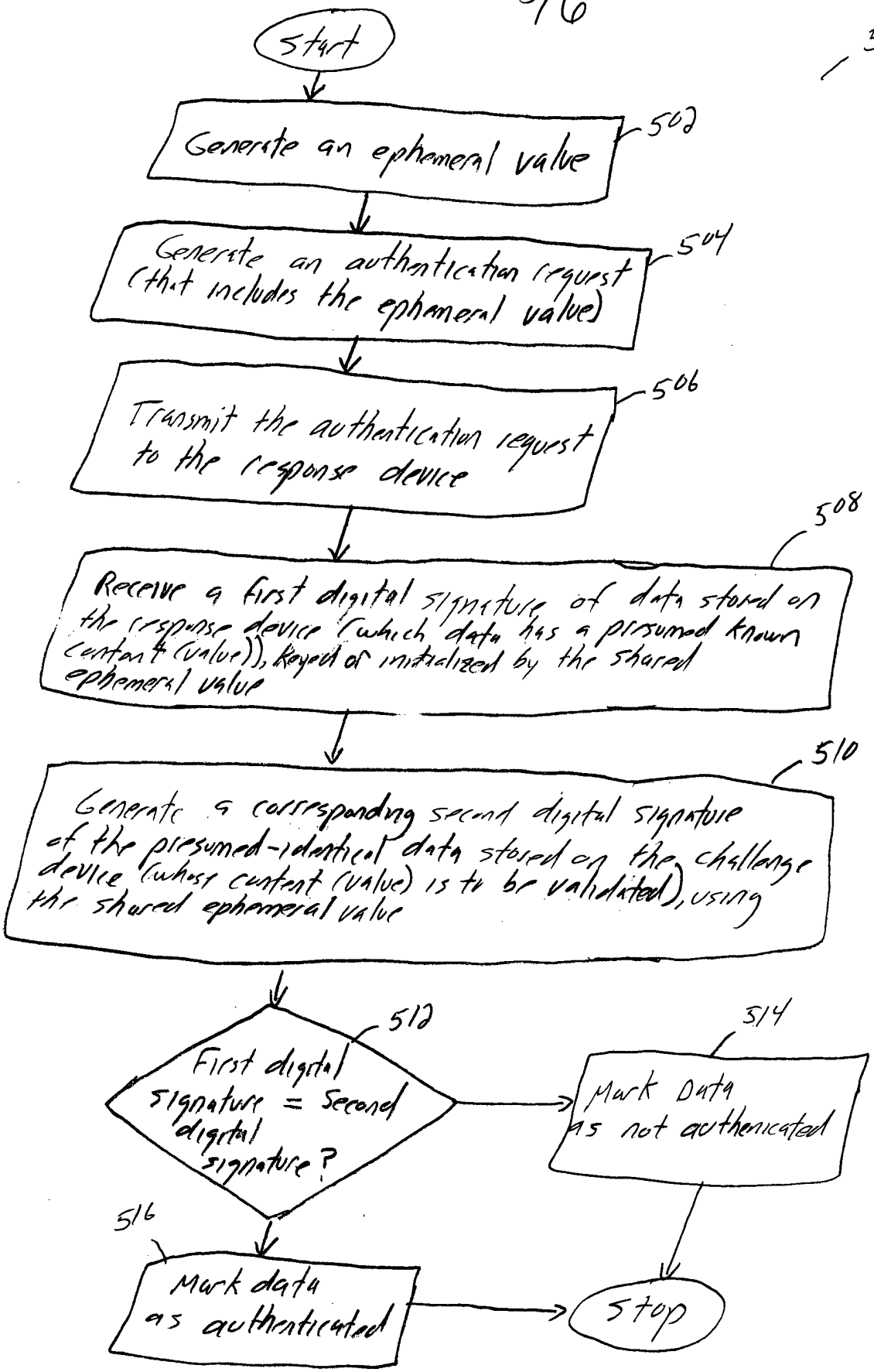
500
Start
Generate an ephemeral value
502
Generate an authentication request (that includes the ephemeral value)
504
Transmit the authentication request to the response device
506
Receive a first digital signature of data stored on the response device (which data has a presumed known content (value)), keyed or initialized by the shared ephemeral value
508
Generate a corresponding second digital signature of the presumed-identical data stored on the challenge device (whose content (value) is to be validated), using the shared ephemeral value
510
First digital signature = Second digital signature?
512
Mark Data as not authenticated
514
Mark data as authenticated
516
Stop

FIG. 5

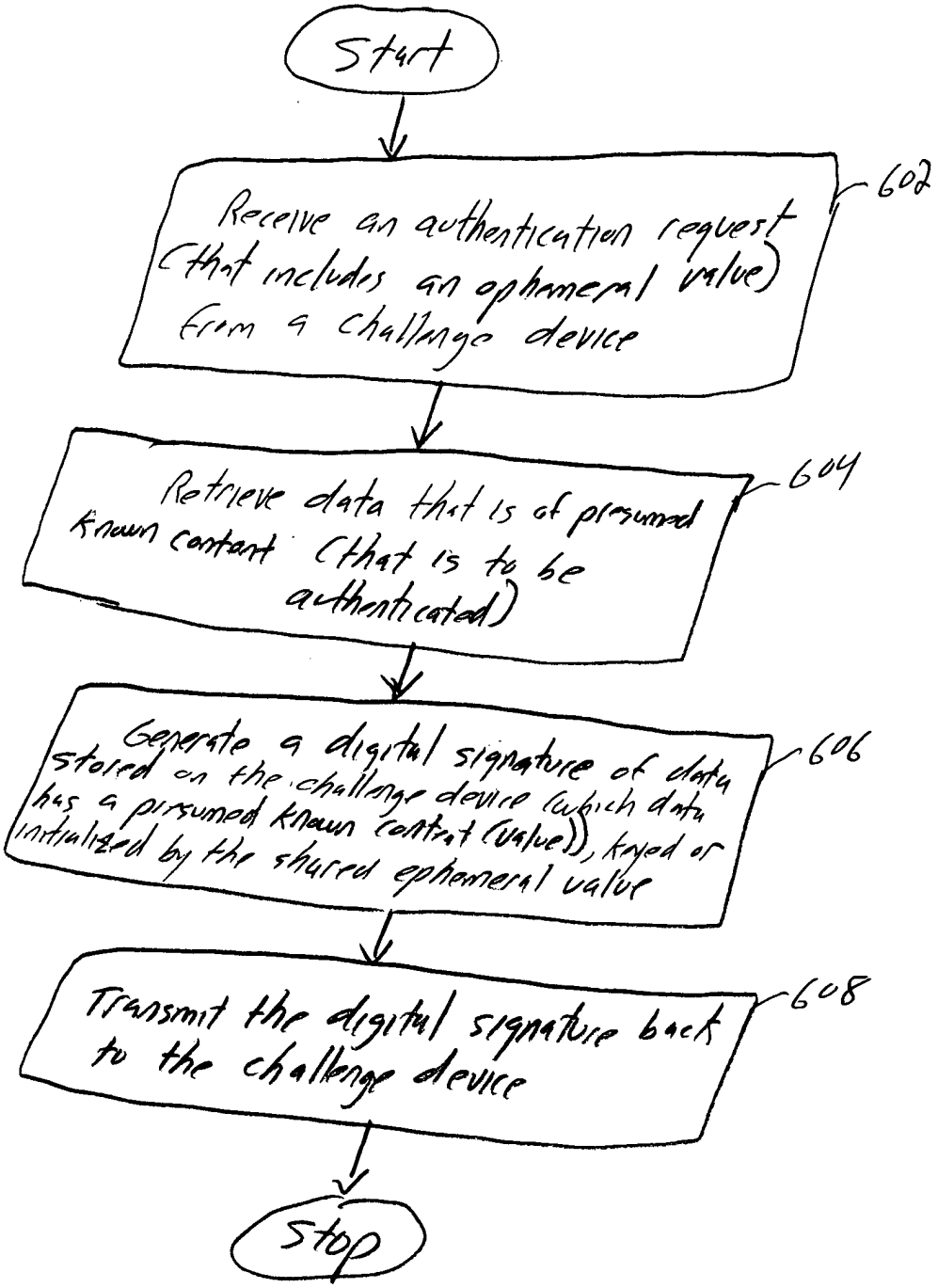
600
Start
Receive an authentication request (that includes an ephemeral value) from a challenge device
602
Retrieve data that is of presumed known content (that is to be authenticated)
604
Generate a digital signature of data stored on the challenge device (which data has a presumed known content (value)), keyed or initialized by the shared ephemeral value
606
Transmit the digital signature back to the challenge device
608
Stop

FIG. 6